305th MI Battalion

Information Security
AR 380-5

Terminal Learning Objective

ACTION: Identify principles of protecting classified information, material and media.

CONDITIONS: Given simulated classified documents or electronic media and AR 380-5.

STANDARDS: Identify principles of protecting classified Information, Material and Media IAW AR 380-5 by achieving 80% on a culminating examination.

Administrative Data

SAFETY REQUIREMENTS: NONE

RISK ASSESSMENT LEVEL: LOW

ENVIROMENTAL CONSIDERATIONS: NONE

EVALUATION: Student will be evaluated by use of Practical Exercises, Student Checks, Homework and pass Information Security Exam with 80% accuracy.

Agenda

ELO A: Annotate Classification Markings to a Document

ELO B: Apply Procedures for Protecting Classified Information

ELO C: Provide Information about Operation Security and the World Wide Web

Enabling Learning Objective A

ACTION: Annotate the Proper Classification Markings to Documents and/or Media.

CONDITIONS: Given AR 380-5, classroom instruction and simulated classified document/media.

STANDARD: Annotate simulated classified documents and/or media by achieving 12 of 15 answers correctly on given performance objective IAW AR 380-5.

ELO Agenda

ELO A: Annotate Classification Markings to Documents/Media

- Classification Process
- Classification Criteria
- Document Markings
- Declassification Programs

Classification Designations

AR 380-5, page 10, para 2-10

Confidential - Cause *Damage*

Secret - Cause *Serious Damage*

Top Secret - Cause *Exceptionally Grave Damage*

To National Security.

Classification Process

page 9, para 2-7

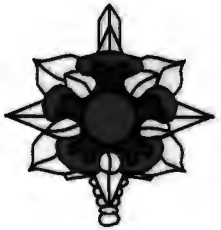
In making a decision to originally classify an item of information, an original classification authority will:

a. Determine that the information has not already been classified

b. Determine that the information is eligible for classification

c. Determine that classification of the information is a realistic course of action and that information can be protected from unauthorized disclosure when classified.

d. Decide that unauthorized disclosure could reasonably be expected to cause damage to national security.



Classification Process (continued)

page 9, para 2-7

e. Select the appropriate level or category of classification and/or sensitivity to be applied to the information, based on a judgment as to the degree of damage unauthorized disclosure could cause

f. Determine and include appropriate declassification, downgrading, and/or exemption instructions to be applied to the information.

g. Make sure that the classification decision is properly communicated so that the information will receive appropriate protection.

Classification Criteria

page 9, para 2-8

- Military Plans, Weapons Systems, or Operations
- Foreign Government Information
- Intelligence Activities, sources or methods
- Foreign Relations Or Activities Of The US
- Scientific, Technological, Or Economic Matters Relating To National Security
- US Government Programs For Safeguarding Nuclear Materials Or Facilities
- Vulnerabilities or capabilities of systems, installations, projects or plans relating to national security

Prohibitions and Limitations

page 9-11, para 2-8, 2-15

- Conceal violations of law, inefficiency, or administrative error
- Prevent embarrassment to a Person, Agency or Organization
- Restrain competition

US classification can only be applied to information that is owned by, produced by or for, or is under the control of the US government.

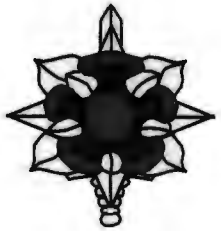
Document Marking

page 23, para 4-4 thru 4-10

Markings will include:

- **Highest level of classification of information contained in the document.**
- **Caveats, when necessary**
- **Classified By:**
- **Reason:**
- **Declassification On:**
- **Date of Source:**

Be sure to include the information that goes with these 4 items

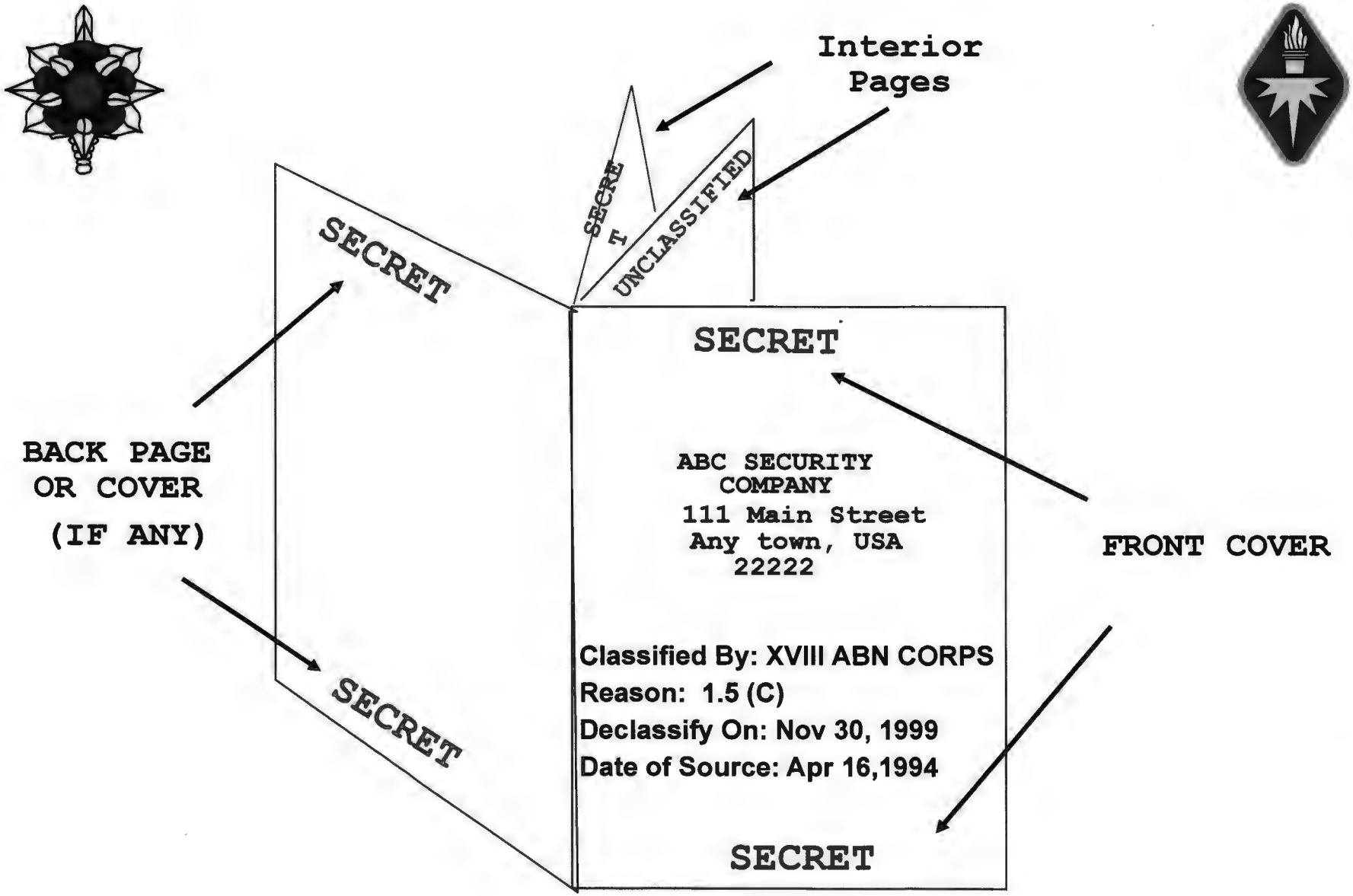


Document Marking

page 22, para 4-4

<u>ALL</u> pages will be marked (centered, top and bottom) with highest classification of information on each page (no abbreviations and capitalized). To include the title page, front page and the front and back of cover pages.

TOP SECRET
SECRET
CONFIDENTIAL
UNCLASSIFIED



Document Marking

page 22, para 4-6

At the beginning of paragraphs and sections will be markings with the appropriate abbreviated classification in parenthesis such as:

(TS) for **TOP SECRET**

(S) for **SECRET**

(C) for **CONFIDENTIAL**

(U) for **UNCLASSIFIED**

DOCUMENT MARKING/CAVEATS

page 23, para 4-6

Examples of Paragraph and Portion Markings:

- **(S/NOFORN) – Secret, No Foreign Nationals**
- **(TS/REL NATO) – Top Secret, Releasable to NATO**
- **(TS/REL GBR) – Top Secret, Releasable to Great Britain**

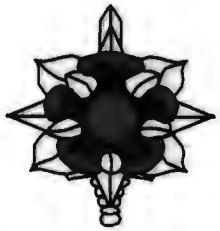
****Notice the single slash between the Classification and the caveat****

Unclassified Document Marking

Unclassified material that is used for training will be clearly marked showing they are UNCLASSIFIED.

An appropriate statement will be placed on the top and bottom of each page.

- **"UNCLASSIFIED"**
- **"FOR TRAINING PURPOSES ONLY"- FTPO**
- **"FOR OFFICIAL USE ONLY"- FOUO**



Unknown Document Marking

Material that is produced by an individual, suspected to be classified but not offered any guidance must be marked with:

"Classification Determination Pending. Protect at Appropriate Classification Level."

STUDENT

[redacted] 5

Subject: Sample of Unclassified subject line [redacted] 1

1. [redacted] 2 For training purposes this paragraph contains Secret information. It must be marked accordingly.

2. [redacted] For training purposes this paragraph contains Confidential information and is for US personnel only. Reason: 1.5(a), mark accordingly.

[redacted] 101st ABN DIV
Reason: 1.5(a)
Declassify on: 26 March 2024
Date of Source: 26 March 1999

[redacted] 5

CHECK

TOP SECRET

Subject: Sample of Unclassified subject line **(U)**

1.(TS) For training purposes this paragraph contains Top Secret information. It must be marked accordingly.

2. **(C)** For training purposes this paragraph contains Confidential information. It must be marked accordingly.

Classified by: G2, 101st ABN DIV
Reason: 1.5(a)
Declassify on: 26 March 2024
Date of Source: 26 March 1999

TOP SECRET

Declassification Programs

page 14, para 3-1

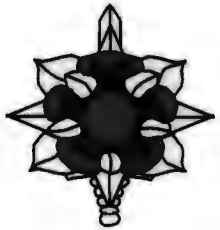
Department of the Army files and records will not be declassified without prior review to determine if continued classification is warranted and authorized.

(1) Original classification authority action

(2) Automatic (Per Executive order)

(3) Mandatory

(4) Systematic



Student Checks

What are 3 unclassified document markings?

UNCLASSIFIED
FOUO
FTPO

What are the 3 classification levels?

Top Secret
Secret
Confidential

QUESTIONS???

Enabling Learning Objective B

ACTION: Apply Procedures for Protecting Classified Information.

CONDITIONS: Given AR 380-5, classroom instruction and simulated classified information and or media.

STANDARD: Applied security regulations and procedures for protecting classified documents and/or media by achieving 12 of 15 answers correctly on given performance objective IAW AR 380-5.

ELO Agenda

ELO B: Apply Procedures for Protecting Classified Information

- General Restrictions for Access
- Accountability and Administrative Procedures
- Storage and Safekeeping of Classified Material
- Identify Methods of Destruction

General Restrictions on Access

page 63, para 6-1

Access Will Be Granted Only When:

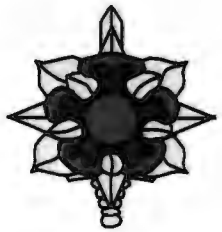
- **Verification of Security Clearance – Joint Personnel Adjudication System (JPAS)**
- **The Person Has A Need-to-know The Information**
- **The Person Has Signed A Nondisclosure Agreement (SF 312)**

Sensitive Compartmented Information

Classified information concerning or derived from intelligence sources, methods or analytical process, which is required to be handled within formal control systems.

The three SCI control systems are:

- **HUMINT, COMINT and TALENT KEYHOLE.**



SCI Control Systems

- **HUMINT-** protects sensitive clandestine HUMINT sources, methods and reporting.
- **COMINT –** protects Electronic Emanations systems and products, a form of Signal Intelligence
    - **GAMMA** – a sub-control Control system
- **TALENT KEYHOLE-** protects satellite recon systems and products/Imagery Intelligence

Determining Responsibility

page 1, para 1-5

Headquarters, Department of the Army (HQDA)-

The Deputy Chief of Staff for Intelligence (DCSINT) is designated as the DA senior official of the Intelligence Community.

- **Direct, administer, and oversee the Army information security program.**
- **Responsible for Information Security matters for units that no longer exist and have no successors.**

Determining Responsibility

page 2, para 1-6, 1-7

The Commander

- Commanders, Officers in Charge, and head of agencies and activities will effectively manage information security programs within their command.
- Commanders may delegate the authority to execute the requirements of AR 380-5, but not the responsibility to do so.

The Command Security Manager-

is the principal advisor to the commander on Information Security.

Individual Responsibility

page 3, para 1-9

- All personnel have an official responsibility to safeguard classified information.

- All personnel will report any violations or anything that could lead to the unauthorized disclosure of classified and sensitive information.

Violations

page 105, para 10-2

- Anyone **FINDING** classified material out of proper control, will take custody of and safeguard the material and immediately notify the Command Security Manager.

- Anyone becoming aware of possible **LOSS** or **COMPROMISE** of classified information will immediately report it to the Command Security Manager.

- Anyone **IDENTIFYING** classified information in the public media, do not make a comment or statement that will confirm or deny the information and immediately notify the Command Security Manager.

Student Check

What are the 3 SCI control Systems?

HUMINT
COMINT
TALENT KEYHOLE

Accountability and Admin Procedures

page 73, para 6-21

Top Secret Information:

- **Provided continuous control and accountability.**
- **Top Secret Control Officers will be designated within offices that hold TS material.**
- **TS material will be accounted for by receipts; held five years.**
- **TS material will be inventoried at least once annually by two properly cleared personnel.**

Accountability and Admin Procedures

page 74, para 6-22

Secret and Confidential Information:

- **Commands will establish procedures to control all Secret and Confidential information IAW AR 380-5.**

- **Material originated, received, distributed, or routed to sub-elements, and information disposed of will be controlled and accounted for.**

Accountability and Admin Procedures

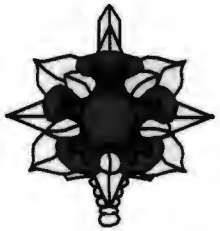
page 74, para 6-24

Working Papers are documents/materials accumulated or created in preparation of finished documents/materials.

- **Papers that contain classified information will be:**
  - **Dated when created.**
  - **Marked as "Draft" or "Working Papers" on the first page.**
  - **Marked with the highest classification of information within the papers.**
  - **Protected in accordance with assigned classification.**
  - **Destroyed when no longer needed.**
  - **Accounted for, controlled, and marked.**

- **180 Day Rule (Review to determine if still needed)**

Storage and Safekeeping



Storage Standards

page 78, para 7-3

Classified information must be secured under adequate conditions to limit access by unauthorized personnel.

- **General Services Administration (GSA) establishes and publishes minimum standards, specifications, and supply schedules for:**
  - **Containers**
  - **Vault Doors**
  - **Alarm Systems**
  - **Associated security devices suitable for storage and protection of classified material.**

Storage and Safekeeping

page 78, para 7-4

Top Secret Material:

- Continuous protection by cleared personnel
- GSA approved security container with one of the following supplemental controls:
  - Cleared/duty personnel will inspect the container once every two hours (no pattern)
  - Intrusion Detection Systems

Secret/Confidential Material:

- GSA approved security container without supplemental controls.

Control Measures

page 67, para 6-9

Commands will maintain measures that ensure access to classified information is limited only to authorized personnel including:

- **Technical (Cameras, Passwords)**
- **Physical (Doors, Guards, Safes)**
- **Administrative (Security Checks)**
- **Personal (Investigations)**
- **Personnel Control (Access Rosters)**

Control Measures

page 67, para 6-9, 6-10

- DA personnel are responsible for ensuring that unauthorized persons do not gain access to classified information.

- Classified information will be protected at all times either by storage, having it under personal observation and physical control of an authorized individual.

Control Measures

page 67, para 6-11

- At the <u>end of the work day</u> a system of security checks will be done to ensure classified material is properly secured.

- The SF 701 (Activity Security Checklist) will be used to record <u>end-of-day</u> security checks.

Control Measures

page 67, para 6-10

Classified document cover sheets will be placed on classified documents or files not in security storage.

- SF 703 (**TOP SECRET** Cover Sheet)
- SF 704 (**SECRET** Cover Sheet)
- SF 705 (**CONFIDENTIAL** Cover Sheet)

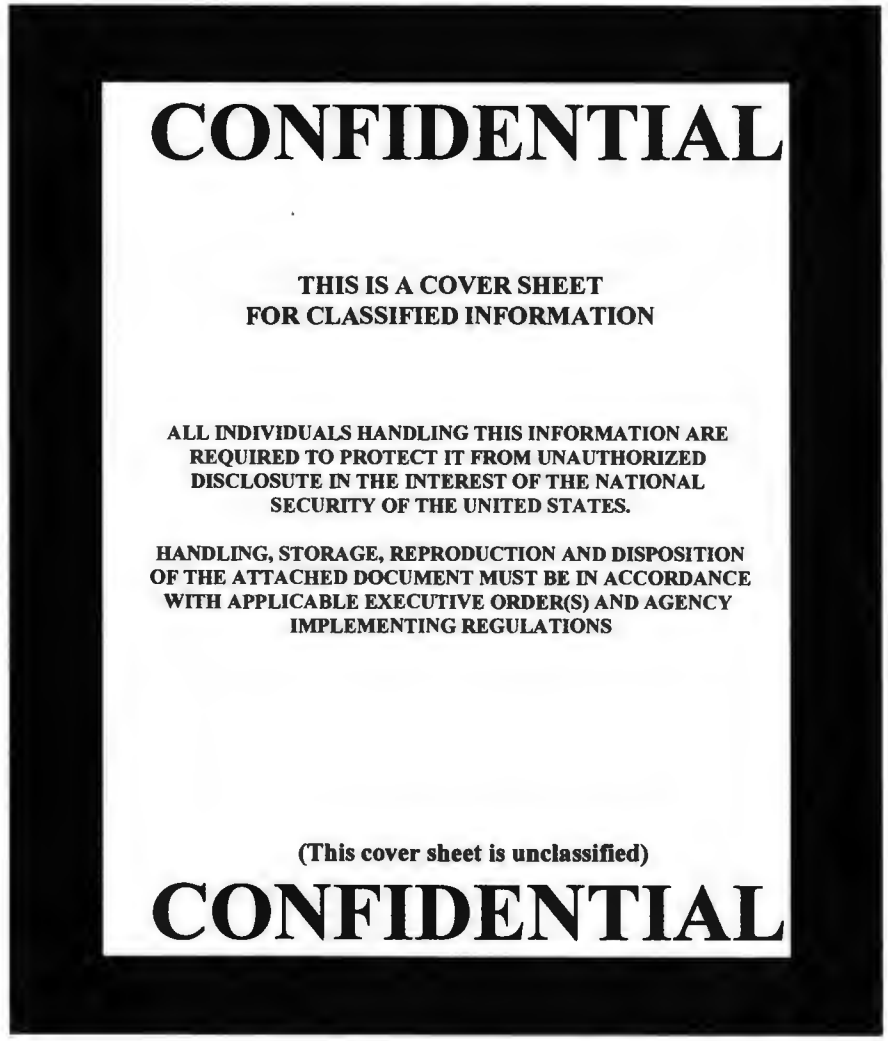
CONFIDENTIAL INFORMATION

SF 705

LOWEST LEVEL OF CLASSIFIED INFORMATON

Paragraph 2-10, AR 380-5

CONFIDENTIAL: Information or material that when disclosed could be expected to cause damage to U.S. security.



SECRET INFORMATION

SF 704

MIDDLE LEVEL OF CLASSIFIED INFORMATON

Paragraph 2-10, AR 380-5

SECRET:
Information or material that when disclosed could be expected to cause serious damage to U.S. security.

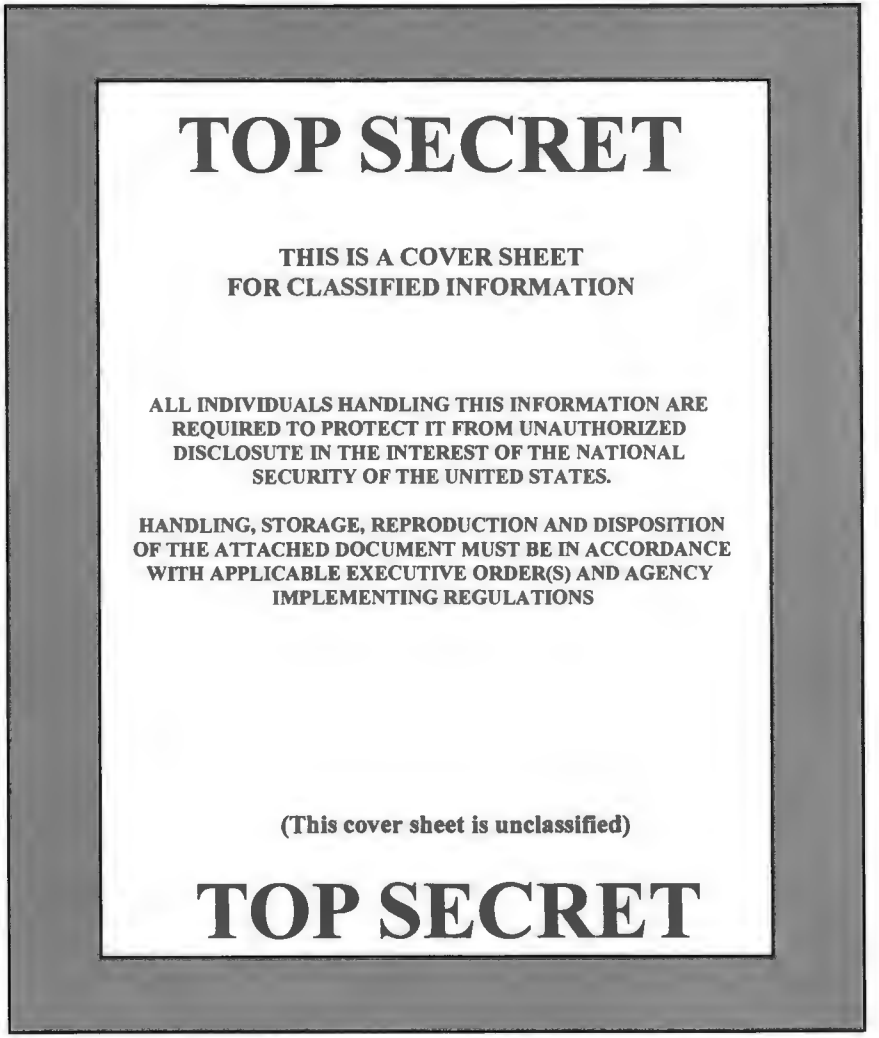
TOP SECRET INFORMATION

SF 703

THE HIGHEST LEVEL OF CLASSIFIED INFORMATION

Paragraph 2-10, AR 380-5

TOP SECRET
Information or material that when disclosed could be expected to cause exceptionally grave damage to U.S. security.



Labeling Computers & Media

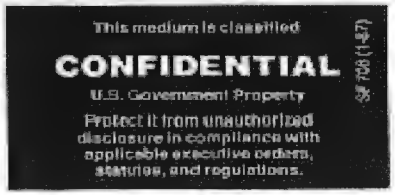
page 31, Section III

- Laptop Computers
- Desktop Computers
- Printers
- Scanners
- Copiers
- Fax Machines
- Disks, Flash Drives, CD's, etc…in a classified environment

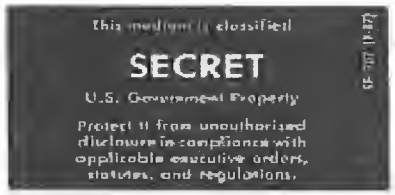
Control Measures

page 33, para 4-34

Classified labels will be placed on all classified Automated Data Processing media

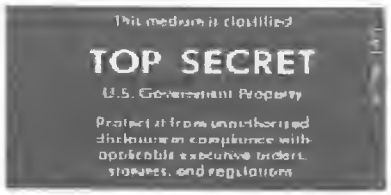


SF 708



SF 707

Others that may be used/seen:



SF 706

SF 711 - Data Descriptor Label
(yellow & black)
SF 712 - CLASSIFIED SCI Label
(yellow & white)

SF 710

Nicknames as a Control Measure

Appendix H, page 212

Nickname – A combination of two separate unclassified words which is assigned an unclassified meaning and is employed only for unclassified administrative, morale or public information purposes.

Operation Iraqi Freedom

Not a correct example of a Nickname!

Student Checks

What are the five control measures to Limit access to classified material?

Technical ↔ Cameras, Passwords
Physical ↔ Doors, Guards, Safes
Administrative ↔ Security Checks
Personal ↔ Investigations
Personnel ↔ Access Rosters

What are some examples?

QUESTIONS???

Transmission/Transportation of Classified Documents

page 90, para 8-2

Top Secret

- Authorized Cryptographic system
- Defense Courier Service
- Authorized or Command courier/messenger service
- Department of State Diplomatic Courier Service
- Cleared U.S. Military personnel, U.S. Government civilian and DOD contractor employees

Transmission/Transportation of Classified Documents

page 90, para 8-3

Secret

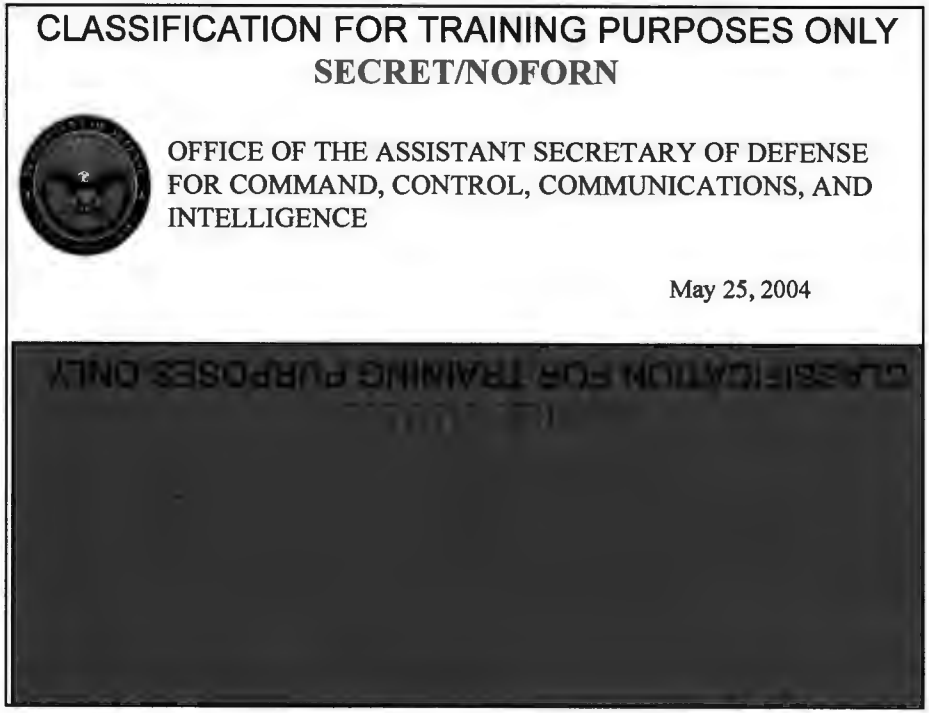
- Any means approved for TOP SECRET
- U.S. Postal Service registered Mail and Express Mail within the 50 states, DC and Puerto Rico
- U.S. Postal Service Registered Mail through Military facilities (APO/FPO) when outside of the U.S and it's territories. As long as it does not pass through foreign postal system or any foreign inspection

Prepare to Mail Classified Documents

page 94, para 8-9/10

- Brown Opaque envelopes
- Packing Tape
- Classification Stamp/Red Pen
- Registered Mail Certificate
- Classified Document receipt (DA Form 3964)
- Classified Document **(SECRET & CONFIDENTIAL only)**
- Inspect the document to ensure that all markings are present and correctly placed on both sides

STEP ONE


CLASSIFICATION FOR TRAINING PURPOSES ONLY
SECRET/NOFORN

OFFICE OF THE ASSISTANT SECRETARY OF DEFENSE
FOR COMMAND, CONTROL, COMMUNICATIONS, AND
INTELLIGENCE

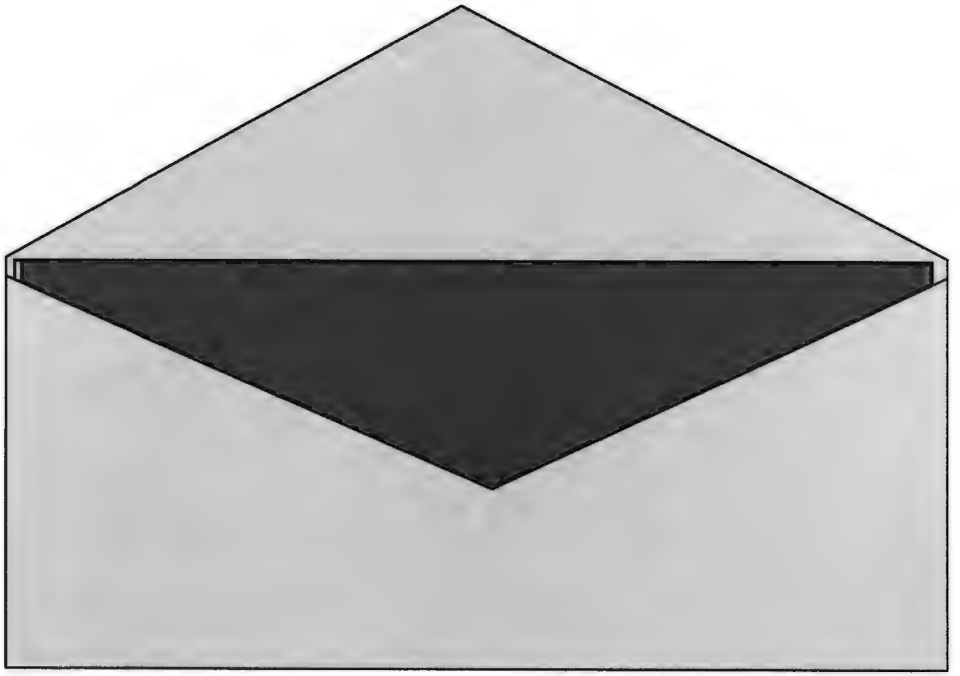
May 25, 2004

- **Document Folded into Thirds**

STEP TWO

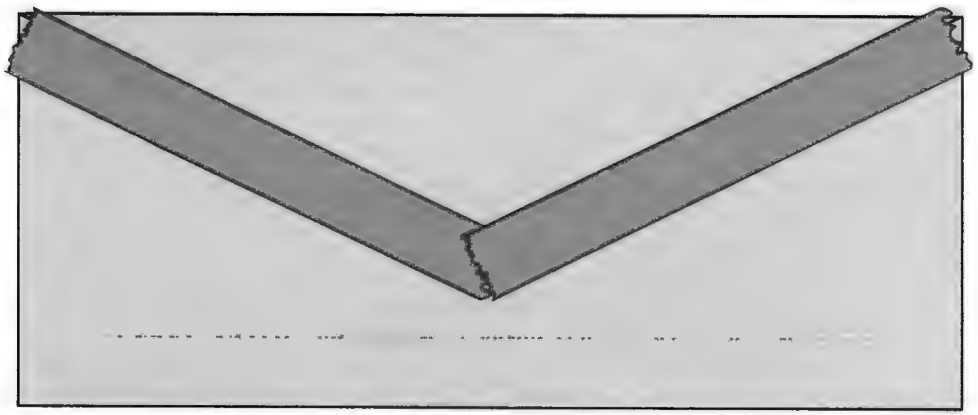
- **Final Folded Document**

STEP THREE



- **Into an Opaque Envelope**

STEP FOUR

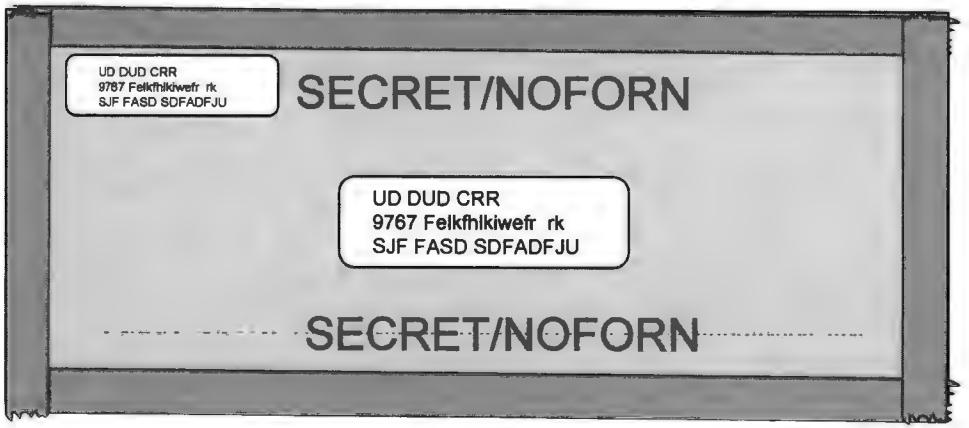


- **Tape Seams**

STEP FIVE

- **Tape Outer Seams**

STEP SIX



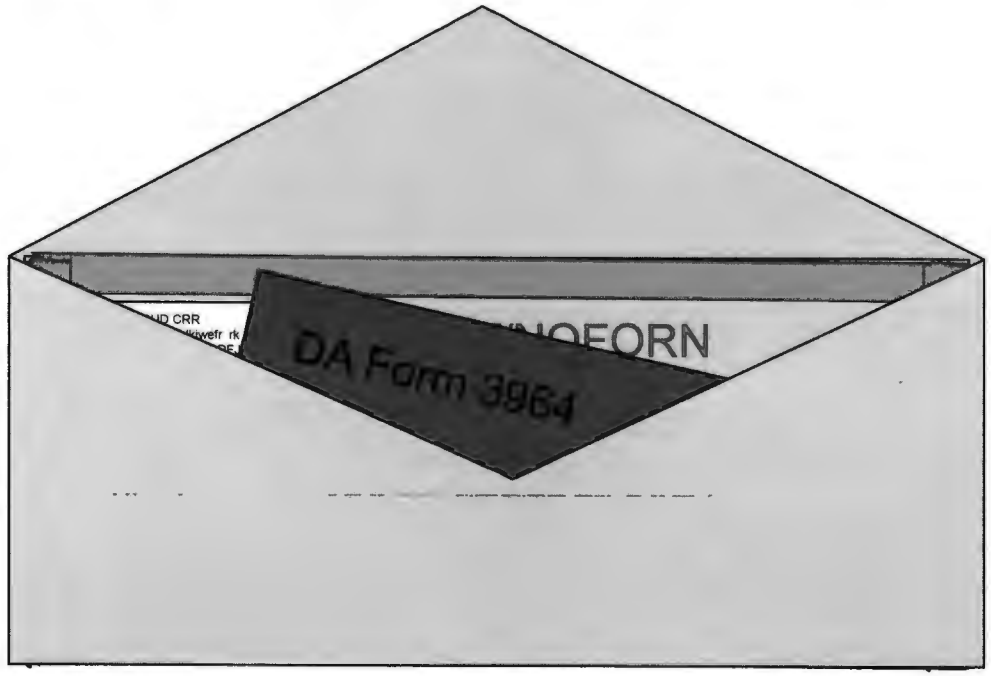
- **Address and Classification Markings**

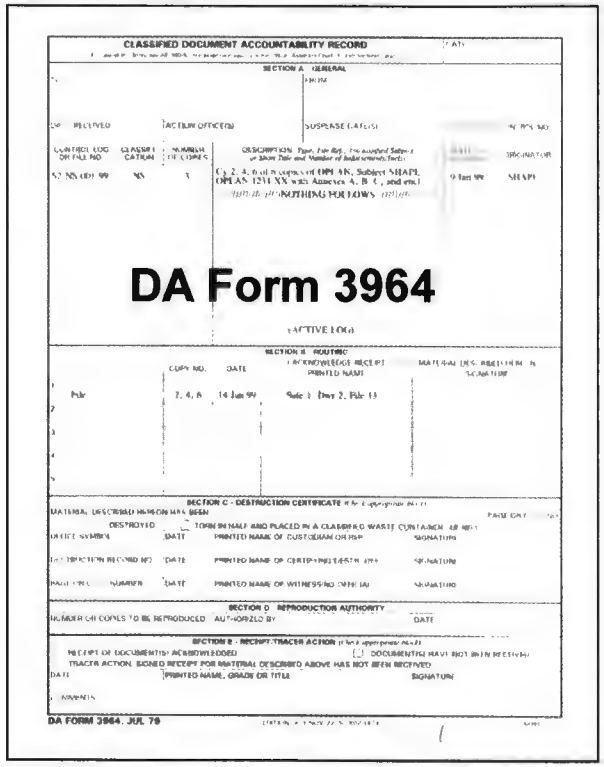
Address/Classification Markings for Inner envelope

page 95, para 8-10b

- Address of sender
- Address of receiving activity - May have Attention line with person's name
- Highest Classification of the contents
- Special Marking such as:
  - "RESRICTED DATA"
  - "NATO"
- Special Instructions- if needed

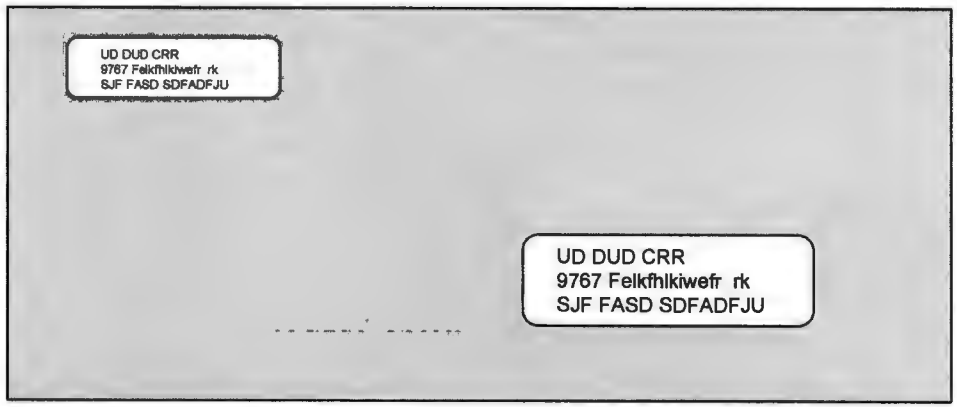
STEP SEVEN





- **Insert a "return" Receipt & Place into the 2nd Envelope (Outer)**

STEP EIGHT



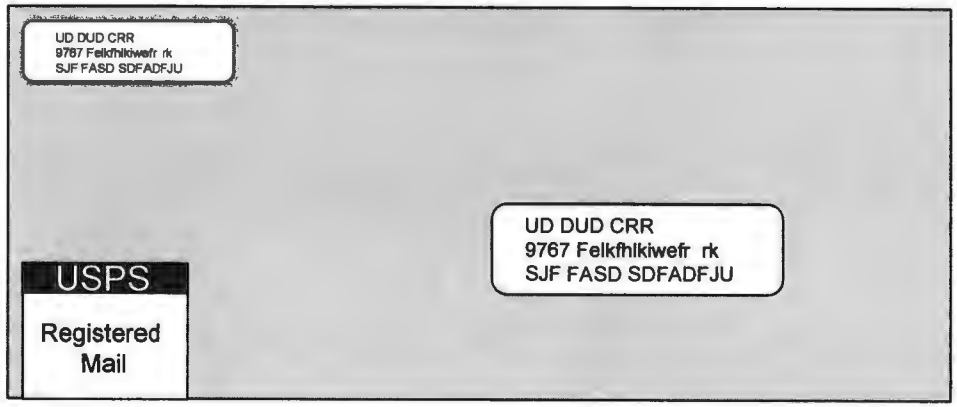
- **Address information**

Address/Marking Information for Outer envelope

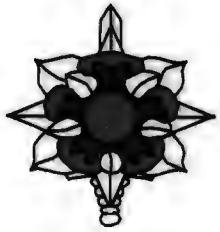
page 95, para 8-10

- Address of sender
- Address of receiving activity such as:
  - Official Government agency/Unit
  - Cleared DOD contractor facility
- May use Office codes or phrases such as
  - "Attention: Research Department"
- May NOT be addressed to an Individual
- Will not bear Classification markings, special markings or any other unusual marks that may draw attention

STEP NINE



- Place in Briefcase and **Lock** Briefcase
- Take to the U.S. Post Office
  - Send Registered Mail
- Wait for Classified Document receipt (DA Form 3964) from receiving agency acknowledging receipt of documents.



Student Check

What classification level can be sent registered mail?

Secret and Below

Methods of Destruction

page 18, para 3-15

- ****<u>Burning</u>**** Preferred method for documents and overlays
- Crosscut Shredding
- Wet Pulping
- Pulverizing

When Destroying CD's, scratch the surface with a key or nail, then break the CD in to several small pieces or burn.

<u>Complete the DA Form3964 (certificate of destruction)</u>

QUESTIONS???

Enabling Learning Objective C

ACTION: Provide Information About Operations Security to the World Wide Web

CONDITIONS: Given Classroom Instruction

STANDARD: Provided a list of aspects related to Operations Security violations on the World Wide Web

ELO Agenda

ELO C: Apply Operations Security to the World Wide Web

- What is Operations Security (OPSEC)
- Different types of critical information
- How to prevent disclosure of critical information

OPSEC

The enemy will attempt to discover how and when we are conducting operations, knowing this, we must protect our activities from detection.

We do this by:

- **Identifying - Critical Information**
- **Analyzing - Threat**

Critical Information

- Photos
- Installation maps with highlights of designated points of interest (sleep/work, CDR, dining facility, etc)
- Security Operating Procedures (SOPs)
- Tactics, Techniques and Procedures (TTPs)
- Unit Capabilities and Intent
- Unit morale
- Personal/Family Information

Sensitive Information

Prevent Disclosure

- **DON'T DISCUSS OPERATIONAL ACTIVITIES ON THE WEB or E-mail**
- **Ensure information posted has no significant value to the adversary**
- **Consider the audience when you're posting to a blog, personal web page or Email**
- **Always assume the adversary is reading your material**
- **Work <u>with</u> your OPSEC Officer – follow policies and procedures!**

<u>Remember it is called the World Wide Web for a reason</u>

Student Checks

What is Critical Information?

It is anything that helps the enemy obtain an advantage over us.

How can we prevent disclosure of Critical Information?

Follow OPSEC Policies & Procedures

Summary

ELO A: Annotate Classification Markings to a Document- Answer 12 of 15 questions correctly

ELO B: Apply Procedures for Protecting Classified Information- Answer 12 of 15 questions correctly

ELO C: Provide information about Operation Security and the World Wide Web - Not tested

QUESTIONS???